

Obsah

Teorie informace	9
1.1. Jednotka informace	9
1.2. Základní pojmy z teorie informace	11
1.3. Přenos informace	13
1.4. Literatura k teorii informace	16
2. Kódování	17
2.1. Základní pojmy z teorie kódů	17
2.1.1. Huffmanova konstrukce nejkratšího kódu	19
2.2. Bezpečnostní kódy	20
2.2.1. Objevování chyb	20
2.2.2. Opravování chyb	21
2.3. Lineární kódy	23
2.3.1. Hammingovy kódy	25
2.4. Cyklické kódy	26
2.4.1. Realizace cyklických kódů	32
2.4.2. Použití cyklických kódů	34
2.5. Kontrolní číslice	36
2.5.1 Rodné číslo	36
2.5.2 Identifikace publikací	37
2.5.3 Čárový kód	38
2.5.4 Identifikační číslo	38
2.5.5 Číslo účtu	39
2.5.6 Identifikační číslo automobilu	39
2.6. Čárové kódy	40
2.7. Literatura ke kódování	42

3. Základy kryptologie	45
3.1. Ochrana informace	45
3.2. Statistické vlastnosti textu.....	46
3.2.1. Abeceda textu.....	46
3.2.2. Zdroj zpráv	47
3.3. Utajený přenos.....	51
3.4. Transpoziční systémy	51
3.4.1. Jednoduchá transpozice.....	52
3.4.2. Šifrovací mřížka	53
3.5. Transkripční systémy.....	55
3.5.1. Monoalfabetické systémy.....	55
3.5.1.1. Systém Cézarovských šifer.....	55
3.5.1.2. Systém afinních šifer.....	57
3.5.1.3. Obecná monoalfabetická šifra	59
3.5.2. Autoklíč.....	63
3.5.3. Polyalfabetické systémy.....	64
3.5.3.1. Vigenérovské šifry	65
3.5.3.2. Polyalfabetická šifra s nekonečným klíčem	69
3.6. Současné systémy.....	71
3.6.1. Systém DES.....	73
3.6.2. Systém RC4 – Rivest Cipher.....	76
3.6.3. Systém AES.....	77

3.7. Systémy s veřejným klíčem.....	78
3.7.1. Binární bitová složitost.....	78
3.7.2. Principy systémů s veřejným klíčem.	80
3.7.3. Architektura systému s veřejným klíčem.....	81
3.7.4. Systém Diffie-Hellman	82
3.7.5. Systém RSA	82
3.8. Literatura ke kryptologii	87
4. Kompresie dat.....	89
4.1. Metoda opakování znaků	89
4.2. Výkonné systémy komprese.....	90
4.2.1. Algoritmus Lempel-Ziv 1977	92
4.2.2. Algoritmus Lempel-Ziv-Welch 1984	94
4.2.3. Huffmanův kód	98
4.2.4. Aritmetická komprese	99
4.3. Kompresie obrazu.....	101
4.4. Literatura ke kompresi dat	102
Rejstřík.....	103